



PERSONVERNOMBUDET I FOLLDAL-ALVDAL-RENDALEN-TOLGA-TYNSET

**Personvernombudet (PVO)
i kommunene
Folldal-Alvdal-Rendalen-Tolga-Tynset**

**Årsmelding
2024**



Innholdsfortegnelse

Om personvernombudet og rapporteringen	3
Generelt om behandling av personopplysninger og ansvar	3
Generelle momenter og tiltak	3
Sikkerhetsforståelse blant de ansatte	3
Tilgjengelighet til systemer uten å være på arbeidsplassen	4
Økt bruk av skytjenester	4
Noen generelle tiltak	4
Avvik meldes til Datatilsynet (DT)	4
Fokusområder på personvernombudet som må videreføres i 2024	5
Personvernombudets tilgang til å melde avvik på vegne av kommunene	5
Avvikshåndtering	5
Få på plass et Internkontrollsystem for IKT-sikkerhet og personvern som tilfredsstiller regelverket i alle FARTT-kommunene	5
Databehandleravtaler og Personvernkonsekvensvurderinger (DPIA`er)	5
Gjennomføring av risikovurderinger og personvernkonsekvensvurderinger (DPIA) før anskaffelser av nye it-systemer som innbefatter behandling av personopplysninger	5
Opplæring av alle ansatte i IKT-sikkerhet og personvern	6
Avslutning	6



Om personvernombudet og rapporteringen

Personvernombudets hovedoppgave er å informere og gi råd om de forpliktelsene virksomheten har etter personvernlovgivningen til den behandlingsansvarlige (øverste leder, kommunedirektøren) eller databehandleren (drifter av datasystemet), samt til de ansatte i kommunene som utfører behandling av personopplysninger. Personvernombudet (PVO) fungerer også som kontaktperson og rådgiver for spørsmål om behandling av personopplysninger og de rettigheter den enkelte registrerte har etter personopplysningsregelverket. PVO er også kontaktperson for kommunene overfor Datatilsynet.

Personombudets rolle kan kort oppsummeres slik:

- Skal bidra til å utvikle en «ryggmargsrefleks for personvern» hos ledere og ansatte
- Kommer vi dit at **alle tenker: «her tror jeg det er noe personverngreier - best vi undersøker litt!»**, da har vi kommet langt!

Personvernombudet skal gi skriftlig rapport til kommunedirektørene i kommunene om arbeidet foregående kalenderår innen 1. mars hvert år. Det utarbeides en felles rapport til alle FARTT-kommunene. Rapporten legges også fram for styret i IKT Fjellregionen IKS til orientering.

Personvernombudet er medlem i IKT-sikkerhetsutvalget i FARTT og samarbeider tett med dette utvalget om problemstillinger omkring til personvern.

Generelt om behandling av personopplysninger og ansvar

God informasjonssikkerhet og søkelys på personvern blir stadig viktigere i dagens samfunn. Alle muligheter og fleksibilitet som elektronisk samhandling gir, skaper også utfordringer omkring personvern for både ledere, brukere, driftsteknikere og systemleverandører.

Personopplysningsloven inkludert personvernforordningen (GDPR) stiller detaljerte og omfattende krav til søkelys på og sikring av informasjon generelt og personopplysninger spesielt. Systemleverandører skal sørge for at datasystemene har innebygget personvern i sin oppbygging og ha standardinnstillinger som sikrer personvernet på en best mulig måte. Dette skal sørge for at informasjonssystemene oppfyller personvernprinsippene, og at de ivaretar de registrertes rettigheter.

I kommunen skal kommunedirektøren som den overordnede behandlingsansvarlige for personopplysninger i kommuneorganisasjonen sørge for at regelverket i forhold til personvern overholdes i alle ledd i sin organisasjon. Virksomheten skal ha full oversikt over sin behandling av personopplysninger og skal iverksette de nødvendige tekniske og organisatoriske tiltak som gjør at loven følges. Virksomhetene har ansvar for å dokumentere at de følger loven.

Generelle momenter og tiltak

Sikkerhetsforståelse blant de ansatte

Parallelt med at mulighetene for forenklet elektronisk samhandling og informasjonshåndtering øker blir også behovet for at de ansatte tar ansvar for egne handlinger stadig mer gjeldende.

Her kan det virke som at teknologien løper litt i forveien, og at ikke alle ansatte helt ser de store sikkerhetsrisikoer dette medfører. Dette kan gjelde ukritisk dokumentlagring, sending av personsensitive data og fødselsnummer i epost, publiseringer, håndtering av elektroniske enheter m.v.



PERSONVERNOMBUDET I FOLLDAL-ALVDAL-RENDALEN-TOLGA-TYNSET

En kommuneorganisasjon består av mange ulike faggrupper av medarbeidere og mange ulike arbeidsoppgaver skal løses. I de forskjellige sektorene og enhetene, og blant de ansatte, vil det være forskjellig hvilke holdninger og normer som er fremtredende i forhold til sikkerhet. Dette må ledelsen være bevisst på og ta hensyn til ved opplæring og oppfølging av den enkelte ansatte og grupper av ansatte i IKT-sikkerhet og personvern. Mer om dette kan lese på [Digdir.no](https://digdir.no). Her finnes også en [interessant \(og morsom\) plakat som beskriver de forskjellige personlighetstypene](#) man kan finne i kommuneorganisasjonen og deres holdninger i forhold til IKT-sikkerhet m.v.

Tilgjengelighet til systemer uten å være på arbeidsplassen

Mange av de ansatte har tjenstlig behov for at systemtilgang skal bli mer tilgjengelig, da med tanke på tilgang fra egne enheter og bruk av systemene når de ikke er på arbeidsplassen. Utvalgte ansatte (ledere og nøkkelpersonell) med spesielle behov for tilgang til systemer kan gis tilgang til intern sone og sikker sone på kommunalt eid bærbar PC utenfor arbeidsstedet (hjemme, på reiser mv). Dette forutsetter bruk godkjente løsninger for sterk autentisering for å høyne sikkerheten.

Fra januar 2025 innføres bruk av sikkerhetsnøkkel for alle ansatte i FARTT-kommunene, både for innlogging på kontoret og utenfor kontoret, noe som bedrer sikkerheten betydelig.

Økt bruk av skytjenester

Det er en gjennomgående trend at flere og flere IKT-systemer som også vi i kommunene bruker blir skybasert. Da vil ikke dataoverføring, dataprosessering og datalagring skje i IKT Fjellregionens serverpark, men fra eksterne serverparker tilknyttet internett et annet sted i Norge eller i Europa. Noen store aktører behandler data også i andre land, som bl a USA. Dette medfører spesielle utfordringer personvernmessig da de har et annet lovverk på området enn EU/EØS.

Noen generelle tiltak

Ved bruk av skytjenester må det sørges for gode databehandleravtaler med skytjenesteleverandørene som sikrer at all data og personopplysninger behandles trygt og sikkert i samsvar med norsk lovgivning.

Grundig opplæring av system-brukerne vil være en nøkkelfaktor for å heve sikkerhetsnivået betydelig. Opplæringen bør i tillegg til dedikert system-opplæring også baseres på generell utøvelse av god sikkerhetskultur samt forståelse av risikobildet og forståelse av risiko ved egne handlinger.

Behovet vil til enhver tid endres og opplæring vil til tider kanskje måtte utføres som intensive opplæringsbolker som kommer parallelt med endringer i sikkerhets- og trusselbildet. Tett dialog mellom IT-drift, ledere, faggrupper og personvernombudet vil også være essensielt for godt sikkerhetsarbeid.

På arbeidsplassen skal alle sørge for at plassering av pc-skjermer er slik at ingen andre enn brukeren selv kan se skjermen, låsing av skjermen og døra når kontoret forlates, ikke la utskrifter bli liggende på skriveren, og å forhindre at uvedkommende får tilgang til fysiske posthyller er enkle og selvfølgelig tiltak for å forbedre sikkerheten.

Avvik meldes til Datatilsynet (DT)

Brudd på personopplysningssikkerheten skal varsles som avvik til Datatilsynet (DT). PVO er gitt tilgang til å varsle slike avvik til DT på vegne av alle FARTT-kommunene (via Altinn).

Brudd på personopplysningssikkerheten kategoriseres i:



PERSONVERNOMBUDET I FOLLDAL-ALVDAL-RENDALEN-TOLGA-TYNSET

1. **Brudd på konfidensialitet**, det vil si at det har vært en utilsiktet eller ulovlig utlevering av eller tilgang til personopplysninger.
2. **Brudd på integritet**, det vil si at det har vært en utilsiktet eller ulovlig endring av personopplysninger.
3. **Brudd på tilgjengelighet**, det vil si der det har vært et utilsiktet eller ulovlig tap av tilgang til eller tilintetgjøring av personopplysninger.

Personvernombudets tilgang til å melde avvik på vegne av kommunene

Kommunedirektørene i alle FARTT-kommunene har gitt personvernombudet nødvendig tilgang til å melde avvik på personvernområdet på vegne av den enkelte kommune. Avvik meldes til Datatilsynet via Altinn. PVO skal holde kommunedirektøren kontinuerlig orientert når avvik blir meldt.

I 2021 ble det meldt 3 avvik til Datatilsynet fra FARTT-kommunene. Det ble ikke registrert avvik i 2022 og 2023 i noen av FARTT-kommunene, men i 2024 er det meldt inn et avvik til DT fra alle 5 kommunene.. Det gjaldt feil oppstått ved FEIDE-innlogging som elever og lærere på skolen bruker.

Avvikshåndtering

Det er utarbeidet en rutine for avviksmelding og håndtering av avvik som skjer på personvernområdet. «Prosedyre for avviksbehandling personvernsaker» ligger tilgjengelig i Compilo i alle 5 kommunene.

Fokusområder på personvernområdet som må videreføres i 2025

Arbeidet med å ivareta personvernet på en best mulig i henhold til lovverket er en prosess som må pågå kontinuerlig og det er viktig å ha et konstant søkelys på dette temaet.

Arbeidet videre vil måtte foregå skrittvis for å få innfridd alle pålagte krav som kommunene skal oppfylle. Arbeid med Personvernkonsekvens-vurderinger (DPIA) og ajourføring av Behandlingsprotokoller må prioriteres. IKT-sikkerhet og personvern i skolene har det blitt fokusert ekstra på i 2024 og dette arbeidet må videreføres i 2025.

Få på plass et Internkontrollsystem for IKT-sikkerhet og personvern som tilfredsstillende regelverket i alle FARTT-kommunene

FARTT-kommunene har i 2023 gått til anskaffelse av Compilos system for Internkontroll GDPR.

IKT-sikkerhetsgruppa i FARTT er i samarbeid godt i gang med arbeidet med å få på plass og ajourført all dokumentasjon, prosedyrer, protokoller m.v. som skal inngå i systemet.

Det bør tas sikte på at systemet er ajouført og godt nok i henhold til kravene i regelverket i løpet av 1. halvår 2025.

Databehandleravtaler og Personvernkonsekvensvurderinger (DPIA`er)

Den enkelte kommune må følge opp arbeidet med å ha signerte databehandleravtaler med alle driftere av IKT-systemene sine på plass, og ha avtalene lagret på en sikker og oversiktlig måte i saksbehandlingssystemet ACOS WebSak+. Alle gjennomførte DPIA`er må også arkiveres på en sikker og oversiktlig måte i ACOS WebSak+.

Gjennomføring av risikovurderinger og personvernkonsekvensvurderinger (DPIA) før anskaffelser av nye it-systemer som innbefatter behandling av personopplysninger

Hver gang kommunen planlegger å ta i bruk et nytt IKT-system har kommunedirektøren ansvaret for at det foretas en vurdering av konsekvensene for personvernet til de personene som får



PERSONVERNOMBUDET I FOLLDAL-ALVDAL-RENDALEN-TOLGA-TYNSET

opplysninger om seg lagret og behandlet i det nye systemet. Det må arbeides videre i 2025 med at med at prosedyrer/rutiner for nyanskaffelser følges av *alle* slik at risiko for personvernet blir tilstrekkelig vurdert **før** nye systemer anskaffes/tas i bruk.

Opplæring av alle ansatte i IKT-sikkerhet og personvern

Kommunedirektøren skal kunne dokumentere at alle ansatte som behandler personopplysninger i sitt arbeid har fått nødvendig opplæring i IKT-sikkerhet og personvern.

KS-læring har et godt e-læringsprogram, «KINS-kurs- Informasjonssikkerhet og personvern», som lagrer dokumentasjon om hvem som har gjennomført programmet

FARTT-kommunene er godt i gang med å gjennomføre dette opplæringsprogrammet for sine ledere og ansatte. Det varierer en del hvor langt den enkelte kommune har kommet i gjennomføringen av opplæringsprogrammet.

KS har på slutten av 2023 lansert en ny kampanje om informasjonssikkerhet og personvern for ansatte i kommuner og fylkeskommuner. Målet med prosjektet er å utløse en «refleks» hos ansatte som gjør at sikkerhet er noe som faller helt naturlig i den digitaliserte hverdagen. Kampanjen har bestått av ti temaer – der ett tema ble rullet ut per måned i totalt ti måneder i 2024. Hver måned har hatt et klart budskap, og målet var å sikre at de kommuneansatte endrer vaner. Alle FARTT-kommune har kjørt dette programmet i 2024.

Avslutning

Personvernombudet kontaktes jevnlig av ansatte, ledere og innbyggere med spørsmål omkring vern av personopplysninger.

Problemstillinger det har vært mye søkelys på for Personvernombudet og IKT-sikkerhetsutvalget som det skal jobbes videre med i 2025 er:

- Personvern omkring bruk av Chromebook og Googles tjenester i skolen. Her må vi følge opp KS sitt arbeid med nasjonal DPIA for Google Workspace for Education
- Få redusert omfanget av sending av fødselsnummer og sensitive opplysning via vanlig ukryptert epost
- Opplæring og dokumentasjon av opplæring i IKT-sikkerhet og Personvern. Fortsatt ha trykk på gjennomføring av programmet i KS-læring for alle ansatte.
- Få ajourført og kvalitetssikret internkontrollsystemet for IKT-sikkerhet og Personvern i Compilo innen 1.juli 2025 til i alle FARTT- kommunene.

Fra 01.12.2024 trer Ole Peter Lindsø inn som nytt Personvernombud for alle FARTT-kommunene.

Tolga 07.01.2025

Kjetil Brodal

PVO i FARTT-kommunene t.o.m. 30.11.2024

epost pvo@fartt.no

tlf 416 00 264